

Docket No. 198274US2TTC/vdm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kouya TOCHIKUBO, et al.

GAU:

SERIAL NO: 09/679,541

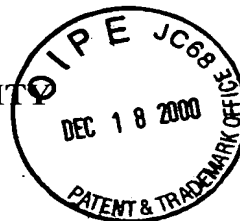
EXAMINER:

FILED: October 6, 2000

FOR: ENCRYPTION ALGORITHM MANAGEMENT SYSTEM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231



SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

APPLICATION NUMBER

MONTH/DAY/YEAR

JAPAN

11-301842

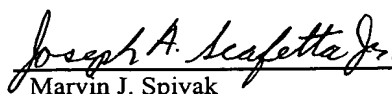
October 25, 1999

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

SSG312630SA1

09/679,541

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

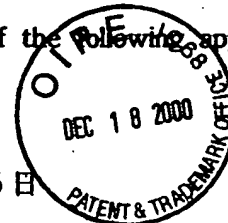
1999年10月25日

出 願 番 号
Application Number:

平成11年特許願第301842号

出 願 人
Applicant(s):

株式会社東芝



CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 9月29日

特許庁長官
Commissioner,
Patent Office

及川耕造

出証番号 出証特2000-3080502

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝

【書類名】 特許願

【整理番号】 A009905265

【提出日】 平成11年10月25日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明の名称】 暗号方式管理システム

【請求項の数】 16

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 枡窪 孝也

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 岡田 光司

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 遠藤 直樹

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書
【発明の名称】 暗号方式管理システム
【特許請求の範囲】

【請求項 1】 暗号化された暗号アルゴリズムを使用可能とするための共通鍵を互いに共有するセンタ装置と端末装置とを備えた暗号方式管理システムであって、

前記端末装置は、

前記暗号化された暗号アルゴリズムを復号する毎に、この暗号化された暗号アルゴリズムを使用可能とする暗号化データを得るためのデータ要求を前記センタ装置に送信する要求送信手段と、

前記要求送信手段のデータ要求に応じて前記センタ装置から暗号化データを受けたとき、前記共通鍵を更新し、この更新された共通鍵に基づいて、前記暗号化データを復号し、得られた復号結果に基づいて前記暗号アルゴリズムを出力する暗号方式管理手段とを有し、

前記センタ装置は、

前記要求送信手段から前記データ要求を受けたとき、前記共有した共通鍵を前記暗号方式管理手段による更新結果と同一に更新する鍵更新手段と、

前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段と

を備えたことを特徴とする暗号方式管理システム。

【請求項 2】 請求項 1 に記載の暗号方式管理システムにおいて、

前記暗号方式管理手段は、前記暗号アルゴリズムの出力に代えて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を出力することを特徴とする暗号方式管理システム。

【請求項 3】 請求項 1 に記載の暗号方式管理システムにおいて、

前記暗号化手段は、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化することを特徴とする暗号方式管理システム。

【請求項 4】 暗号化された暗号アルゴリズムを使用可能とするための共通

鍵をセンタ装置と互いに共有する端末装置であって、

前記暗号化された暗号アルゴリズムを復号する毎に、この暗号化された暗号アルゴリズムを使用可能とする暗号化データを得るためのデータ要求を前記センタ装置に送信する要求送信手段と、

前記要求送信手段のデータ要求に応じて前記センタ装置から暗号化データを受けたとき、前記共通鍵を更新し、この更新された共通鍵に基づいて、前記暗号化データを復号し、得られた復号結果に基づいて前記暗号アルゴリズムを出力する暗号方式管理手段と

を備えたことを特徴とする端末装置。

【請求項 5】 請求項 4 に記載の端末装置において、

前記暗号方式管理手段は、前記暗号アルゴリズムの出力に代えて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を出力することを特徴とする端末装置。

【請求項 6】 請求項 4 又は請求項 5 に記載の端末装置において、

前記暗号方式管理手段は、外部から書換不可能で且つ内部を読込めない記憶領域にあることを特徴とする端末装置。

【請求項 7】 暗号化された暗号アルゴリズムを使用可能とするための共通鍵を端末装置と互いに更新可能に共有するセンタ装置であって、

前記端末装置からデータ要求を受けたとき、前記共有した共通鍵を端末装置による更新結果と同一に更新する鍵更新手段と、

前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段と

を備えたことを特徴とするセンタ装置。

【請求項 8】 請求項 7 に記載のセンタ装置において、

前記暗号化手段は、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化することを特徴とするセンタ装置。

【請求項 9】 請求項 7 又は請求項 8 に記載のセンタ装置において、

前記端末装置からデータ要求を受けたとき、前記端末装置に対して暗号アルゴ

リズムの使用権限の有無を判定し、使用権限が有るときのみ、前記鍵更新手段に前記更新を実行させる使用権限判定手段を備えたことを特徴とするセンタ装置。

【請求項 1 0】 暗号化された暗号アルゴリズムを使用可能とするための共通鍵を互いに共有するセンタ装置と端末装置とを備えた暗号方式管理システムであって、

前記端末装置は、

前記暗号化された暗号アルゴリズムを復号する際に、今回の累積復号回数が所定回数以下のときには前記共通鍵を更新せずに前記暗号アルゴリズムを復号可能とし、今回の累積復号回数が所定回数を越えるときには前記共通鍵を更新して前記暗号アルゴリズムを復号不可とする暗号方式管理手段と、

前記暗号方式管理手段により共通鍵が更新されたとき、前記更新された共通鍵で前記暗号アルゴリズムを使用可能とするためのデータ要求を前記センタ装置に送信する要求送信手段とを有し、

前記センタ装置は、

前記要求送信手段から前記データ要求を受けたとき、前記共有した共通鍵を前記暗号方式管理手段による更新結果と同一に更新する鍵更新手段と、

前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段と

を備えたことを特徴とする暗号方式管理システム。

【請求項 1 1】 請求項 1 0 に記載の暗号方式管理システムにおいて、

前記暗号化手段は、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化することを特徴とする暗号方式管理システム。

【請求項 1 2】 暗号化された暗号アルゴリズムを使用可能とするための共通鍵をセンタ装置と互いに共有する端末装置であって、

前記暗号化された暗号アルゴリズムを復号する際に、今回の累積復号回数が所定回数以下のときには前記共通鍵を更新せずに前記暗号アルゴリズムを復号可能とし、今回の累積復号回数が所定回数を越えるときには前記共通鍵を更新して前記暗号アルゴリズムを復号不可とする暗号方式管理手段と、

前記暗号方式管理手段により共通鍵が更新されたとき、前記更新された共通鍵で前記暗号アルゴリズムを使用可能とするためのデータ要求を前記センタ装置に送信する要求送信手段と

を備えたことを特徴とする端末装置。

【請求項 1 3】 請求項 1 2 に記載の端末装置において、
前記暗号方式管理手段は、外部から書換不可能で且つ内部を読込めない記憶領域にあることを特徴とする端末装置。

【請求項 1 4】 暗号化された暗号アルゴリズムを使用可能とするための共通鍵を端末装置と互いに更新可能に共有するセンタ装置であって、

前記端末装置からデータ要求を受けたとき、前記共有した共通鍵を前記端末装置による更新結果と同一に更新する鍵更新手段と、

前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段と

を備えたことを特徴とするセンタ装置。

【請求項 1 5】 請求項 1 4 に記載のセンタ装置において、
前記暗号化手段は、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化することを特徴とするセンタ装置。

【請求項 1 6】 請求項 1 4 又は請求項 1 5 に記載のセンタ装置において、
前記端末装置からデータ要求を受けたとき、前記端末装置に対して暗号アルゴリズムの使用権限の有無を判定し、使用権限が有るときのみ、前記鍵更新手段に前記更新を実行させる使用権限判定手段を備えたことを特徴とするセンタ装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、暗号方式利用システムで使用する暗号アルゴリズムを管理し、暗号方式の不正利用を阻止し得る暗号方式管理システムに関する。

【0 0 0 2】

【従来の技術】

現在、ネットワークに接続されている様々な機器では、機密を保持する観点から、暗号アルゴリズム及び鍵による暗号方式を利用した暗号方式利用システムが広く用いられている。この種の暗号方式利用システムでは、様々な暗号アルゴリズムが存在し、それらの暗号アルゴリズムは、夫々用途に応じて使い分けされている。

【0003】

係る暗号アルゴリズムは、その鍵長などによっては米国等において輸出が規制されている。しかしながら、この種の暗号アルゴリズムは、オープンなネットワークの発達により、正当権限の無い者に不正利用される現状にある。

【0004】

【発明が解決しようとする課題】

以上説明したように、従来の暗号方式利用システムは、オープンなネットワークの発達により、暗号アルゴリズムが不正利用されている現状にある。

【0005】

本発明は上記実情を考慮してなされたもので、暗号方式利用システムに用いられる暗号アルゴリズムを管理し、暗号アルゴリズムの不正利用を阻止し得る暗号方式管理システムを提供することを目的とする。

【0006】

【課題を解決するための手段】

請求項1に対応する発明は、暗号化された暗号アルゴリズムを使用可能とするための共通鍵を互いに共有するセンタ装置と端末装置とを備えた暗号方式管理システムであって、前記端末装置としては、前記暗号化された暗号アルゴリズムを復号する毎に、この暗号化された暗号アルゴリズムを使用可能とする暗号化データを得るためのデータ要求を前記センタ装置に送信する要求送信手段と、前記要求送信手段のデータ要求に応じて前記センタ装置から暗号化データを受けたとき、前記共通鍵を更新し、この更新された共通鍵に基づいて、前記暗号化データを復号し、得られた復号結果に基づいて前記暗号アルゴリズムを出力する暗号方式管理手段とを有し、前記センタ装置としては、前記要求送信手段から前記データ要求を受けたとき、前記共有した共通鍵を前記暗号方式管理手段による更新結果

と同一に更新する鍵更新手段と、前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段とを備えた暗号方式管理システムである。

【 0 0 0 7 】

また、請求項 2 に対応する発明は、請求項 1 に対応する暗号方式管理システムにおいて、前記暗号方式管理手段としては、前記暗号アルゴリズムの出力に代えて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を出力する暗号方式管理システムである。

【 0 0 0 8 】

さらに、請求項 3 に対応する発明は、請求項 1 に対応する暗号方式管理システムにおいて、前記暗号化手段としては、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化する暗号方式管理システム。

【 0 0 0 9 】

また、請求項 4 に対応する発明は、暗号化された暗号アルゴリズムを使用可能とするための共通鍵をセンタ装置と互いに共有する端末装置であって、前記暗号化された暗号アルゴリズムを復号する毎に、この暗号化された暗号アルゴリズムを使用可能とする暗号化データを得るためのデータ要求を前記センタ装置に送信する要求送信手段と、前記要求送信手段のデータ要求に応じて前記センタ装置から暗号化データを受けたとき、前記共通鍵を更新し、この更新された共通鍵に基づいて、前記暗号化データを復号し、得られた前記暗号アルゴリズムを出力する暗号方式管理手段とを備えた端末装置である。

【 0 0 1 0 】

また、請求項 5 に対応する発明は、請求項 4 に対応する端末装置において、前記暗号方式管理手段としては、前記暗号アルゴリズムの出力に代えて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を出力する端末装置である。

【 0 0 1 1 】

さらに、請求項 6 に対応する発明は、請求項 4 又は請求項 5 に対応する端末装置において、前記暗号方式管理手段としては、外部から書換不可能で且つ内部を

読込めない記憶領域にある端末装置である。

【0012】

また、請求項7に対応する発明は、暗号化された暗号アルゴリズムを使用可能とするための共通鍵を端末装置と互いに更新可能に共有するセンタ装置であって、前記端末装置からデータ要求を受けたとき、前記共有した共通鍵を端末装置による更新結果と同一に更新する鍵更新手段と、前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段とを備えたセンタ装置である。

【0013】

さらに、請求項8に対応する発明は、請求項7に対応するセンタ装置において、前記暗号化手段としては、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化するセンタ装置である。

【0014】

また、請求項9に対応する発明は、請求項7又は請求項8に対応するセンタ装置において、前記端末装置からデータ要求を受けたとき、前記端末装置に対して暗号アルゴリズムの使用権限の有無を判定し、使用権限が有るときのみ、前記鍵更新手段に前記更新を実行させる使用権限判定手段を備えたセンタ装置である。

【0015】

さらに、請求項10に対応する発明は、暗号化された暗号アルゴリズムを使用可能とするための共通鍵を互いに共有するセンタ装置と端末装置とを備えた暗号方式管理システムであって、前記端末装置としては、前記暗号化された暗号アルゴリズムを復号する際に、今回の累積復号回数が所定回数以下のときには前記共通鍵を更新せずに前記暗号アルゴリズムを復号可能とし、今回の累積復号回数が所定回数を越えるときには前記共通鍵を更新して前記暗号アルゴリズムを復号不可とする暗号方式管理手段と、前記暗号方式管理手段により共通鍵が更新されたとき、前記更新された共通鍵で前記暗号アルゴリズムを使用可能とするためのデータ要求を前記センタ装置に送信する要求送信手段とを有し、前記センタ装置としては、前記要求送信手段から前記データ要求を受けたとき、前記共有した共通

鍵を前記暗号方式管理手段による更新結果と同一に更新する鍵更新手段と、前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段とを備えた暗号方式管理システムである。

【0016】

また、請求項11に対応する発明は、請求項10に対応する暗号方式管理システムにおいて、前記暗号化手段としては、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化する暗号方式管理システムである。

【0017】

さらに、請求項12に対応する発明は、暗号化された暗号アルゴリズムを使用可能とするための共通鍵をセンタ装置と互いに共有する端末装置であって、前記暗号化された暗号アルゴリズムを復号する際に、今回の累積復号回数が所定回数以下のときには前記共通鍵を更新せずに前記暗号アルゴリズムを復号可能とし、今回の累積復号回数が所定回数を越えるときには前記共通鍵を更新して前記暗号アルゴリズムを復号不可とする暗号方式管理手段と、前記暗号方式管理手段により共通鍵が更新されたとき、前記更新された共通鍵で前記暗号アルゴリズムを使用可能とするためのデータ要求を前記センタ装置に送信する要求送信手段とを備えた端末装置である。

【0018】

また、請求項13に対応する発明は、請求項12に対応する端末装置において、前記暗号方式管理手段としては、外部から書換不可能で且つ内部を読込めない記憶領域にある端末装置である。

【0019】

さらに、請求項14に対応する発明は、暗号化された暗号アルゴリズムを使用可能とするための共通鍵を端末装置と互いに更新可能に共有するセンタ装置であって、前記端末装置からデータ要求を受けたとき、前記共有した共通鍵を前記端末装置による更新結果と同一に更新する鍵更新手段と、前記鍵更新手段により更新された共通鍵に基づいて、前記暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化し、得られた暗号化データを前記端末装置に返信する暗号化手段と

を備えたセンタ装置である。

【0020】

また、請求項15に対応する発明は、請求項14に対応するセンタ装置において、前記暗号化手段としては、前記復号鍵の暗号化に代えて、前記暗号アルゴリズムを暗号化するセンタ装置である。

【0021】

さらに、請求項16に対応する発明は、請求項14又は請求項15に対応するセンタ装置において、前記端末装置からデータ要求を受けたとき、前記端末装置に対して暗号アルゴリズムの使用権限の有無を判定し、使用権限が有るときのみ、前記鍵更新手段に前記更新を実行させる使用権限判定手段を備えたセンタ装置である。

【0022】

(作用)

従って、請求項1～5, 7, 8に対応する発明は以上のような手段を講じたことにより、端末装置としては、要求送信手段が、暗号化された暗号アルゴリズムを復号する毎に、この暗号化された暗号アルゴリズムを使用可能とする暗号化データを得るためのデータ要求をセンタ装置に送信し、センタ装置としては、鍵更新手段が、要求送信手段からデータ要求を受けたとき、共有した共通鍵を暗号方式管理手段による更新結果と同一に更新し、暗号化手段が、鍵更新手段により更新された共通鍵に基づいて、暗号化された暗号アルゴリズムを復号可能な復号鍵あるいは暗号アルゴリズム自体を暗号化し、得られた暗号化データを端末装置に返信し、端末装置としては、暗号方式管理手段が、要求送信手段のデータ要求に応じてセンタ装置から暗号化データを受けたとき、共通鍵を更新し、この更新された共通鍵に基づいて、暗号化データを復号し、得られた暗号化された暗号アルゴリズムを復号可能な復号鍵あるいは暗号アルゴリズム自体を出力する。

【0023】

このように、端末装置が暗号アルゴリズムを使用する毎に、センタ装置から暗号化データを得る必要がある構成としたので、暗号方式利用システムに用いられる暗号アルゴリズムを管理でき、暗号アルゴリズムの不正利用を阻止することが

できる。

【 0 0 2 4 】

また、請求項 6 に対応する発明は、暗号方式管理手段が、外部から書換不可能で且つ内部を読込めない記憶領域にあるので、請求項 4, 5 に対応する作用に加え、悪意の第三者による改ざんを阻止することができる。

【 0 0 2 5 】

さらに、請求項 9 に対応する発明は、使用権限判定手段が、端末装置からデータ要求を受けたとき、端末装置に対して暗号アルゴリズムの使用権限の有無を判定し、使用権限が有るときのみ、鍵更新手段に更新を実行させるので、請求項 7, 8 に対応する作用に加え、端末装置の使用権限に基づいて、暗号アルゴリズムを管理することができる。

【 0 0 2 6 】

また、請求項 1 0 ~ 1 2, 1 4, 1 5 に対応する発明は、端末装置としては、暗号方式管理手段が、暗号化された暗号アルゴリズムを復号する際に、今回の累積復号回数が所定回数以下のときには共通鍵を更新せずに前記暗号アルゴリズムを復号可能とし、今回の累積復号回数が所定回数を越えるときには共通鍵を更新して暗号アルゴリズムを復号不可とし、要求送信手段が、暗号方式管理手段により共通鍵が更新されたとき、更新された共通鍵で暗号アルゴリズムを使用可能とするためのデータ要求をセンタ装置に送信し、センタ装置としては、鍵更新手段が、要求送信手段からデータ要求を受けたとき、共有した共通鍵を暗号方式管理手段による更新結果と同一に更新し、暗号化手段が、鍵更新手段により更新された共通鍵に基づいて、暗号化された暗号アルゴリズムを復号可能な復号鍵あるいは暗号アルゴリズム自体を暗号化し、得られた暗号化データを端末装置に返信する。

【 0 0 2 7 】

このように、端末装置が暗号アルゴリズムを使用する毎に、使用回数をカウントし、有効な使用回数を過ぎた暗号アルゴリズムを無効化させる構成としたので、暗号方式利用システムに用いられる暗号アルゴリズムを管理でき、暗号アルゴリズムの不正利用を阻止することができる。

【 0 0 2 8 】

また、請求項 1 3 に対応する発明は、暗号方式管理手段が、外部から書換不可能で且つ内部を読込めない記憶領域にあるので、請求項 1 2 に対応する作用に加え、悪意の第三者による改ざんを阻止することができる。

【 0 0 2 9 】

さらに、請求項 1 6 に対応する発明は、使用権限判定手段が、端末装置からデータ要求を受けたとき、端末装置に対して暗号アルゴリズムの使用権限の有無を判定し、使用権限が有るときのみ、鍵更新手段に更新を実行させるので、請求項 1 4, 1 5 に対応する作用に加え、端末装置の使用権限に基づいて、暗号アルゴリズムを管理することができる。

【 0 0 3 0 】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照して説明する。

なお、本実施形態において、 $E(X)[y]$, $E(Z,X)[y]$ は、元データ y が暗号アルゴリズム z を用いて共通鍵 x で暗号化された暗号化データを表している。

【 0 0 3 1 】

(第 1 の実施形態)

図 1 は本発明の第 1 の実施形態に係る暗号方式管理システムの構成を示すブロック図である。この暗号方式管理システムは、センタ装置 1 0 が通信路を介して n 個の端末装置 2 0 i に接続された構成となっている。

【 0 0 3 2 】

ここで、センタ装置 1 0 は、制御部 1 1、線形フィードバックシフトレジスタ 1 2、鍵情報格納部 1 3 及び暗号化部 1 4 を備えている。

【 0 0 3 3 】

制御部 1 1 は、端末装置 2 0 i から要求を受けたとき、例えば有効期限等の管理情報に基づいて端末装置 2 0 i が暗号アルゴリズムを使用可能な否か（＝使用権限の有無）を判定し、使用可能なとき（＝使用権限有のとき）、端末装置 2 0 i 内の暗号アルゴリズム管理部 2 3 における線形フィードバックシフトレジスタ 1 2 の状態値 t を自センタの線形フィードバックシフトレジスタ 1 2 に入力する

と共に、暗号アルゴリズムの識別情報IDA1を鍵情報格納部13に入力する機能をもっている。

【0034】

線形フィードバックシフトレジスタ12は、制御部11から入力された状態値 t に基づいて、次の状態値 Kt を生成し、得られた状態値 Kt を暗号化部14に入力する機能をもっている。

【0035】

鍵情報格納部13は、識別情報IDA1毎に復号化鍵KA1を保持し、制御部11から入力された識別情報IDA1に対応する復号化鍵KA1を暗号化部14に入力する機能をもっている。

【0036】

暗号化部14は、線形フィードバックシフトレジスタ12からの状態値 Kt に基づいて、鍵情報格納部13からの復号化鍵KA1を暗号化し、得られた暗号化データ $E1(Kt)[KA1]$ を端末装置20iに送信する機能をもっている。

【0037】

一方、端末装置20iは、パソコンの如き計算機等が適宜使用可能となっており、図示するように、鍵情報格納部21、暗号アルゴリズム格納部22、暗号アルゴリズム管理部23及び暗号化・復号化部24を備え、これら各部21～24を制御する機能をもっている。

【0038】

鍵情報格納部21は、図示しない他の端末装置jとの通信用の鍵 Kij が格納されたメモリ領域であり、端末装置20i本体からの制御により、鍵 Kij を暗号化・復号化部24に転送可能となっている。

【0039】

暗号アルゴリズム格納部22は、暗号アルゴリズムA1が暗号化された暗号化データ $E2(KA1)[A1]$ が格納されたメモリ領域であり、端末装置20i本体からの制御により、この暗号化データ $E2(KA1)[A1]$ を暗号アルゴリズム管理部23に転送可能となっている。

【0040】

暗号アルゴリズム管理部 23 は、センタ装置 10 からの暗号化データ $E1(Kt) [KA1]$ を復号する機能を有し、この復号結果 ($KA1$ 又はエラー) に基づいて、暗号アルゴリズム格納部 22 からの暗号化データ $E2(KA1) [A1]$ を復号するものであり、この復号結果 ($A1$ 又はエラー) を暗号化・復号化部 24 に入力する機能をもっている。

【0041】

具体的には、暗号アルゴリズム管理部 23 は、外部から書換不可能で且つ内部を読込めない記憶領域に設けられ、図 2 に示すように、制御部 25、線形フィードバックシフトレジスタ 26、鍵情報復号化部 27 及び暗号アルゴリズム復号化部 28 を備えている。

【0042】

ここで、制御部 25 は、センタ装置 10 から暗号化データ $E1(Kt) [KA1]$ を受け且つ暗号アルゴリズム格納部 22 から暗号化データ $E2(KA1) [A1]$ を受けたとき、鍵 $KA1$ の暗号化データ $E1(Kt) [KA1]$ を鍵情報復号化部 27 に入力すると共に、暗号アルゴリズム $A1$ の暗号化データ $E2(KA1) [A1]$ を暗号アルゴリズム復号化部 28 に入力し、且つ次の状態値の生成信号 “1” を線形フィードバックシフトレジスタ 26 に入力する機能をもっている。

【0043】

線形フィードバックシフトレジスタ 26 は、状態値 t を保持し、制御部 25 から生成信号 “1” を受けると、この状態値 t から次の状態値 Kt を生成し、得られた状態値 Kt を鍵情報復号化部 27 に入力する機能をもっている。

【0044】

鍵情報復号化部 27 は、線形フィードバックシフトレジスタ 26 から受けた状態値 Kt を鍵として、制御部 25 から受けた暗号化データ $E1(Kt) [KA1]$ を復号し、得られた復号結果 $KA1$ を暗号アルゴリズム復号化部 28 に入力する機能をもっている。

【0045】

暗号アルゴリズム復号化部 28 は、鍵情報復号化部 27 から受けた復号結果 $KA1$ を鍵として、制御部 25 から受けた暗号化データ $E2(KA1) [A1]$ を復号し、得ら

れた復号結果A1を暗号化・復号化部24に入力する機能をもっている。

【0046】

暗号化・復号化部24は、暗号アルゴリズム管理部23内の暗号アルゴリズム復号化部28から受けた暗号アルゴリズムA1と、鍵情報格納部21から受けた鍵 K_{ij} とに基づいて、端末装置20本体から入力されるメッセージMを暗号化し、得られた暗号化データ $E(A1, K_{ij})[M]$ を他の端末装置iに送信する機能をもっている。

【0047】

次に、以上のように構成された暗号方式管理システムの動作を説明する。

センタ装置10においては、端末装置20から要求を受けたとき、制御部11が、例えば有効期限等に基づいて端末装置20が暗号アルゴリズムを使用可能な否かを判定し、使用可能なとき、端末装置20内の暗号アルゴリズム管理部における線形フィードバックシフトレジスタ12の状態値tを自センタの線形フィードバックシフトレジスタ12に入力すると共に、暗号アルゴリズムの識別情報ID A1を鍵情報格納部13に入力する。

【0048】

線形フィードバックシフトレジスタ12は、この状態値tに基づいて、次の状態値を生成し、得られた状態値 Kt を暗号化部14に入力する。

【0049】

鍵情報格納部13は、制御部からの識別情報ID A1に対応する復号化鍵KA1を暗号化部14に入力する。

【0050】

暗号化部14は、線形フィードバックシフトレジスタからの状態値 Kt に基づいて、鍵情報格納部からの復号化鍵KA1を暗号化し、得られた暗号化データ $E1(Kt)[KA1]$ を端末装置に送信する。

【0051】

端末装置20においては、暗号化データ $E1(Kt)[KA1]$ の受信により鍵情報格納部21を制御し、鍵情報格納部21内の鍵 K_{ij} が暗号化・復号化部24に転送される。

【0052】

また、暗号アルゴリズム格納部 22 では、端末装置 20 本体からの制御により、この暗号化データ $E2(KA1)[A1]$ が暗号アルゴリズム管理部 23 に転送される。

【0053】

暗号アルゴリズム管理部 23 においては、制御部 25 が、センタ装置 10 から暗号化データ $E1(Kt)[KA1]$ を受け且つ暗号アルゴリズム格納部 22 から暗号化データ $E2(KA1)[A1]$ を受けたとき、鍵 $KA1$ の暗号化データ $E1(Kt)[KA1]$ を鍵情報復号化部 27 に入力すると共に、暗号アルゴリズム $A1$ の暗号化データ $E2(KA1)[A1]$ を暗号アルゴリズム復号化部 28 に入力し、且つ次の状態値の生成信号 “1” を線形フィードバックシフトレジスタ 26 に入力する。

【0054】

線形フィードバックシフトレジスタ 26 は、状態値 t を保持し、制御部 25 から生成信号 “1” を受けると、この状態値 t から次の状態値 Kt を生成し、得られた状態値 Kt を鍵情報復号化部 27 に入力する。

【0055】

鍵情報復号化部 27 は、線形フィードバックシフトレジスタ 26 から受けた状態値 Kt を鍵として、制御部 25 から受けた暗号化データ $E1(Kt)[KA1]$ を復号し、得られた復号結果 $KA1$ を暗号アルゴリズム復号化部 28 に入力する。

【0056】

暗号アルゴリズム復号化部 28 は、鍵情報復号化部 27 から受けた復号結果 $KA1$ を鍵として、制御部 25 から受けた暗号化データ $E2(KA1)[A1]$ を復号し、得られた復号結果 $A1$ を暗号化・復号化部 24 に入力する。

【0057】

暗号化・復号化部 24 は、暗号アルゴリズム管理部 23 内の暗号アルゴリズム復号化部 28 から受けた暗号アルゴリズム $A1$ と、鍵情報格納部 21 から受けた鍵 Kij とに基づいて、端末装置 20 本体から入力されるメッセージ M を暗号化し、得られた暗号化データ $E(A1, Kij)[M]$ を他の端末装置 i に送信する。

【0058】

上述したように本実施形態によれば、端末装置 20 i が暗号アルゴリズム $A1$ を

使用する毎に、暗号アルゴリズムを使用する毎に暗号アルゴリズム復号化鍵が更新され、センタ装置 10 から暗号化データを得る必要がある構成としたので、暗号方式利用システムに用いられる暗号アルゴリズムを管理でき、暗号アルゴリズムの不正利用を阻止することができる。また、この手法は、端末装置 20 i における記憶装置のバックアップによる暗号アルゴリズムの不正利用をも防ぐことができる。

【0059】

また、暗号アルゴリズム管理部 23 が、外部から書換不可能で且つ内部を読込めない記憶領域にあるので、悪意の第三者による改ざんを阻止することができる。

【0060】

さらに、センタ装置 10 の制御部 11 が、端末装置 20 i からデータ要求を受けたとき、端末装置 20 i に対して暗号アルゴリズムの使用権限の有無を判定し、使用権限が有るときのみ、線形フィードバックシフトレジスタ 12 に状態値 t の更新を実行させるので、端末装置 20 i の使用権限に基づいて、暗号アルゴリズムを管理することができる。

【0061】

なお、これら管理部 23 の耐タンパー性による改ざん阻止の効果や制御部 11 による使用権限の判定の効果は、管理部の動作と名称は変わるものの、以下の各実施形態でも同様である。

(第 2 の実施形態)

図 3 は本発明の第 2 の実施形態に係る暗号方式管理システムの構成を示すブロック図であり、図 4 はその暗号アルゴリズム管理部の構成を示すブロック図であって、図 1 及び図 2 と同一要素には同一符号を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。なお、以下の実施形態も同様にして重複した説明を省略する。

【0062】

すなわち、本実施形態は、第 1 の実施形態の変形形態であり、センタ装置側では、鍵の暗号化データに代えて、暗号アルゴリズムの暗号化データを送信する構

成となっており、且つ端末装置側では、暗号アルゴリズムの毎回の使用毎に要求を送信する構成に代えて、暗号アルゴリズムの n 回の使用毎に要求をセンタ装置に送信する構成としている。

【0063】

具体的には、センタ装置 10a では、鍵情報格納部 13 に代えて、暗号アルゴリズム格納部 15 を設けている。

【0064】

また、端末装置 20ia 本体では、センタ装置 10a から送信された、暗号アルゴリズムを含む暗号化データ $E2(Kt)[A1]$ を暗号アルゴリズム格納部 22 に格納する機能を有し、且つ図 2 に示した暗号アルゴリズム管理部 23 に代えて、図 4 に示すように、カウンタを含む暗号アルゴリズム管理部 30 を設けている。

【0065】

ここで、暗号アルゴリズム格納部 15 は、識別情報 $IDA1$ 毎に暗号アルゴリズム $A1$ を保持し、前述同様に、制御部 11 から入力された識別情報 $IDA1$ に対応する暗号アルゴリズム $A1$ を暗号化部 14 に入力する機能をもっている。

【0066】

なお、暗号化部 14 は、線形フィードバックシフトレジスタ 12 からの状態値 Kt に基づいて、暗号アルゴリズム格納部 15 からの暗号アルゴリズム $A1$ を暗号化し、得られた暗号化データ $E2(Kt)[A1]$ を端末装置 20ia に送信する機能をもっている。

【0067】

一方、暗号アルゴリズム管理部 30 は、暗号アルゴリズム格納部 22 から暗号化データ $E2(Kt)[A1]$ が転送されたとき、この転送された回数をカウントしておき、転送回数が n 回以下のときには暗号化データを復号して得られた暗号アルゴリズムを暗号化・復号化部 24 に入力するが、転送回数が n 回を越えたときには復号を失敗させて得たランダムなデータを暗号化・復号化部 24 に入力する機能をもっている。

【0068】

具体的には、暗号アルゴリズム管理部 30 は、外部から書換不可能で且つ内部

を読込めない記憶領域に設けられ、図 4 に示すように、制御部 3 1、カウンタ 3 2、線形フィードバックシフトレジスタ 3 3 及び暗号アルゴリズム復号化部 3 4 を備えている。

【 0 0 6 9 】

ここで、制御部 3 1 は、暗号アルゴリズム格納部 2 2 から暗号化データ $E2(Kt)$ [A1] を受けたとき、暗号アルゴリズム A1 の暗号化データ $E2(Kt)$ [A1] を暗号アルゴリズム復号化部 3 4 に入力し、且つ使用回数信号 “1” をカウンタ 3 2 に入力する機能をもっている。

【 0 0 7 0 】

カウンタ 3 2 は、使用回数を保持し、制御部 3 1 から使用回数信号を受けると、保持する使用回数を + 1 だけ更新し、この更新結果が使用許可の上限回数以下のとき、信号 “0” を線形フィードバックシフトレジスタ 3 3 に入力し、更新結果が使用許可の上限回数を越えるとき、信号 “1” を線形フィードバックシフトレジスタ 3 3 に入力する機能をもっている。

【 0 0 7 1 】

線形フィードバックシフトレジスタ 3 3 は、状態値 Kt を保持し、カウンタ 3 2 から信号 “0” を受けると、この状態値 Kt を暗号アルゴリズム復号化部 3 4 に入力し、カウンタ 3 2 から信号 “1” を受けると、この状態値 Kt から生成した次の状態値 $Kt+1$ を暗号アルゴリズム復号化部 3 4 に入力する機能をもっている。

【 0 0 7 2 】

暗号アルゴリズム復号化部 3 4 は、線形フィードバックシフトレジスタ 3 3 から受けた復号結果 Kt を鍵として、制御部 3 1 から受けた暗号化データ $E2(Kt)$ [A1] を復号し、得られた復号結果 A1 を暗号化・復号化部 2 4 に入力する機能をもっている。なお、暗号アルゴリズム復号化部 3 4 は、線形フィードバックシフトレジスタ 3 3 から復号結果 $Kt+1$ を受けたとき、この $Kt+1$ を鍵として、制御部 3 1 から受けた暗号化データ $E2(Kt)$ [A1] を復号し、復号結果としてランダムなデータ（異なる鍵で復号されて得られたデータ）を暗号化・復号化部 2 4 に入力する機能をもっている。

【 0 0 7 3 】

次に、以上のように構成された暗号方式管理システムの動作を説明する。

センタ装置 10a においては、端末装置 20ia から前述同様に要求をうけたとき、暗号アルゴリズム格納部 15 が、制御部 11 から入力された識別情報 IDA1 に対応する暗号アルゴリズム AI を暗号化部 14 に入力する。

【0074】

暗号化部 14 は、線形フィードバックシフトレジスタ 12 からの状態値 K_t に基づいて、暗号アルゴリズム格納部 15 からの暗号アルゴリズム AI を暗号化し、得られた暗号化データ $E2(K_t)[AI]$ を端末装置 20ia に送信する。

【0075】

端末装置 20ia においては、この暗号アルゴリズムを含む暗号化データ $E2(K_t)[AI]$ を暗号アルゴリズム格納部 22 に格納する。また、暗号アルゴリズムを使用する毎に、暗号アルゴリズム格納部 22 を制御して暗号アルゴリズムを暗号アルゴリズム管理部 23 に転送させる。

【0076】

具体的には、暗号アルゴリズム管理部 30 においては、制御部 31 が、暗号アルゴリズム格納部 22 から暗号化データ $E2(K_t)[AI]$ を受けたとき、暗号アルゴリズム AI の暗号化データ $E2(K_t)[AI]$ を暗号アルゴリズム復号化部 34 に入力し、且つ使用回数信号 “1” をカウンタ 32 に入力する。

【0077】

カウンタ 32 は、制御部 31 から使用回数信号を受けると、保持する使用回数を +1 だけ更新し、この更新結果が使用許可の上限回数以下のとき、信号 “0” を線形フィードバックシフトレジスタ 33 に入力し、更新結果が使用許可の上限回数を越えるとき、信号 “1” を線形フィードバックシフトレジスタ 33 に入力する。

【0078】

線形フィードバックシフトレジスタ 33 は、カウンタ 32 から信号 “0” を受けると、状態値 K_t を暗号アルゴリズム復号化部 34 に入力し、カウンタ 32 から信号 “1” を受けると、この状態値 K_t から生成した次の状態値 K_{t+1} を暗号アルゴリズム復号化部 34 に入力する。

【0079】

暗号アルゴリズム復号化部34は、線形フィードバックシフトレジスタ33から受けた復号結果 K_t を鍵として、制御部31から受けた暗号化データ $E2(K_t)[A1]$ を復号し、得られた復号結果 $A1$ を暗号化・復号化部24に入力する。

【0080】

以下、前述同様に、暗号化・復号化部24では、暗号アルゴリズム管理部30内の暗号アルゴリズム復号化部34から受けた暗号アルゴリズム $A1$ と、鍵情報格納部21から受けた鍵 K_{ij} とに基づいて、端末装置20本体から入力されるメッセージ M を暗号化し、得られた暗号化データ $E(A1, K_{ij})[M]$ を他の端末装置 i に送信する。

【0081】

また、暗号アルゴリズム復号化部34は、線形フィードバックシフトレジスタ33から復号結果 K_{t+1} を受けた場合、この K_{t+1} を鍵として、制御部31から受けた暗号化データ $E2(K_t)[A1]$ を復号し、復号結果としてランダムなデータ（異なる鍵で復号されて得られたデータ）を暗号化・復号化部24に入力する。

【0082】

この場合、暗号化・復号化部24では、メッセージ M を暗号化できず、エラーを出力する。

上述したように本実施形態によれば、暗号アルゴリズム管理部30が、暗号アルゴリズム格納部22から暗号化データ $E2(K_t)[A1]$ が転送されたとき、この転送された回数をカウントしておき、転送回数が n 回以下のときには暗号化データを復号して得られた暗号アルゴリズムを暗号化・復号化部24に入力するが、転送回数が n 回を越えたときには復号を失敗させて得たランダムなデータを暗号化・復号化部24に入力する。

【0083】

このように、端末装置20iaが暗号アルゴリズムを使用する毎に、使用回数をカウントし、有効な使用回数を過ぎると、暗号アルゴリズムを復号化するための鍵が更新されて暗号アルゴリズムを無効化させる構成としたので、暗号方式利用システムに用いられる暗号アルゴリズムを管理でき、暗号アルゴリズムの不正

利用を阻止することができる。また、この手法は、端末装置における記憶装置のバックアップによる暗号アルゴリズムの不正利用をも防ぐことができる。

【0084】

(第3の実施形態)

図5は本発明の第3の実施形態に係る暗号方式管理システムの構成を示すブロック図であり、図6はその暗号アルゴリズム管理部の構成を示すブロック図である。

【0085】

すなわち、本実施形態は、第1の実施形態の変形形態であり、端末装置側では、復号化鍵の毎回の使用毎に要求を送信する構成に代えて、復号化鍵のn回の使用毎に復号化の要求をセンタ装置に送信する構成としている。

【0086】

具体的には、端末装置20i本体では、センタ装置10から送信された、復号化鍵を含む暗号化データ $E1(Kt)[KA1]$ を鍵情報格納部21bに格納する機能を有し、且つ図2に示した暗号アルゴリズム管理部23に代えて、図4に示すように、カウンタを含む鍵情報管理部40を設けている。

【0087】

鍵情報格納部21bは、通信用の鍵 Kij の暗号化データ $E1(Ki)[Kij]$ の格納機能に加え、センタ装置から送信された復号化鍵の暗号化データ $E1(Kt)[KA1]$ が格納され、端末装置20i本体からの制御により、暗号化データ $E1(Kt)[KA1]$ 及び $E1(Ki)[Kij]$ を鍵情報管理部40に転送可能となっている。

【0088】

鍵情報管理部40は、暗号アルゴリズム格納部22から暗号化データ $E1(Kt)[KA1]$ 及び $E1(Ki)[Kij]$ が転送されたとき、通信用の鍵 Kij の暗号化データ $E1(Ki)[Kij]$ を復号して得られた鍵 Kij を暗号化・復号化部24に与える一方、暗号アルゴリズムの鍵 $KA1$ の暗号化データ $E1(Kt)[KA1]$ の転送された回数をカウントしておき、転送回数がn回以下のときには暗号化データを復号して得られた復号鍵 $KA1$ を暗号アルゴリズム復号化部28bに入力するが、転送回数がn回を越えたときには復号を失敗させて得たランダムなデータを暗号アルゴリズム復号化部2

8 b に入力する機能をもっている。

【 0 0 8 9 】

具体的には、鍵情報管理部 4 0 は、外部から書換不可能で且つ内部を読込めない記憶領域に設けられ、図 6 に示すように、鍵情報制御部 4 1、第 1 の鍵情報復号化部 4 2、カウンタ 4 3、線形フィードバックシフトレジスタ 4 4 及び第 2 の鍵情報復号化部 4 5 を備えている。

【 0 0 9 0 】

ここで、鍵情報制御部 4 1 は、鍵情報格納部 2 1 b から暗号化データ $E1(Kt) [KA1]$ 及び $E1(Ki) [Kij]$ を受けたとき、暗号化データ $E1(Ki) [Kij]$ を第 1 の鍵情報復号化部 4 2 に入力すると共に、暗号化データ $E1(Kt) [KA1]$ を第 2 の鍵情報復号化部 4 5 に入力し、且つ使用回数信号 “1” をカウンタ 4 3 に入力する機能をもっている。

【 0 0 9 1 】

第 1 の鍵情報復号化部 4 2 は、鍵情報制御部 1 4 から入力された暗号化データ $E1(Ki) [Kij]$ を端末固有の鍵 Ki で復号化し、得られた通信用の鍵 Kij を暗号化・復号化部 2 4 に入力する機能をもっている。

【 0 0 9 2 】

カウンタ 4 3 は、使用回数を保持し、鍵情報制御部 4 1 から使用回数信号を受けると、保持する使用回数を + 1 だけ更新し、この更新結果が使用許可の上限回数以下のとき、信号 “0” を線形フィードバックシフトレジスタ 4 4 に入力し、更新結果が使用許可の上限回数を越えるとき、信号 “1” を線形フィードバックシフトレジスタ 4 4 に入力する機能をもっている。

【 0 0 9 3 】

線形フィードバックシフトレジスタ 4 4 は、状態値 Kt を保持し、カウンタ 4 3 から信号 “0” を受けると、この状態値 Kt を第 2 の鍵情報復号化部 4 5 に入力し、カウンタ 4 3 から信号 “1” を受けると、この状態値 Kt から生成した次の状態値 $Kt+1$ を第 2 の鍵情報復号化部 4 5 に入力する機能をもっている。

【 0 0 9 4 】

第 2 の鍵情報復号化部 4 5 は、線形フィードバックシフトレジスタ 4 4 から受

けた復号結果 K_t を鍵として、鍵情報制御部 41 から受けた暗号化データ $E_1(K_t)[KA_1]$ を復号し、得られた復号結果 KA_1 を暗号アルゴリズム復号化部 28b に入力する機能をもっている。なお、第 2 の鍵情報復号化部 45 は、線形フィードバックシフトレジスタ 44 から復号結果 K_{t+1} を受けたとき、この K_{t+1} を鍵として、鍵情報制御部 41 から受けた暗号化データ $E_1(K_t)[KA_1]$ を復号し、復号結果としてランダムなデータ（異なる鍵で復号されて得られた失敗データ）を暗号アルゴリズム復号化部 28b に入力する機能をもっている。

【0095】

暗号アルゴリズム復号化部 28b は、第 2 の鍵情報復号化部 45 から受けた復号結果 KA_1 を鍵として、暗号アルゴリズム格納部 22 から受けた暗号化データ $E_2(KA_1)[A_1]$ を復号し、得られた復号結果 A_1 を暗号化・復号化部 24 に入力する機能をもっている。

【0096】

次に、以上のように構成された暗号方式管理システムの動作を説明する。

センタ装置 10 においては、端末装置 20ib から前述同様に要求をうけたとき、復号化鍵の暗号化データ $E_1(K_t)[KA_1]$ を端末装置 20ib に送信する。

【0097】

端末装置 20ib においては、この暗号化データ $E_1(K_t)[KA_1]$ を暗号アルゴリズム格納部 22 に格納する。また、暗号アルゴリズムを使用する毎に、暗号アルゴリズム格納部 22 を制御して暗号化データ $E_1(K_t)[KA_1]$ 及び $E_1(K_i)[K_{ij}]$ を鍵情報管理部 40 に転送させる。

【0098】

鍵情報管理部 40 においては、鍵情報制御部 41 が、暗号化データ $E_1(K_t)[KA_1]$ 及び $E_1(K_i)[K_{ij}]$ を受けたとき、暗号化データ $E_1(K_i)[K_{ij}]$ を第 1 の鍵情報復号化部 42 に入力すると共に、暗号化データ $E_1(K_t)[KA_1]$ を第 2 の鍵情報復号化部 45 に入力し、且つ使用回数信号“1”をカウンタ 43 に入力する。

【0099】

第 1 の鍵情報復号化部 42 は、入力された暗号化データ $E_1(K_i)[K_{ij}]$ を端末固有の鍵 K_i で復号化し、得られた通信用の鍵 K_{ij} を暗号化・復号化部 24 に入力す

る。

【0100】

一方、カウンタ43は、使用回数信号を受けると、保持する使用回数を+1だけ更新し、この更新結果が使用許可の上限回数以下のとき、信号“0”を線形フィードバックシフトレジスタ44に入力し、更新結果が使用許可の上限回数を越えるとき、信号“1”を線形フィードバックシフトレジスタ44に入力する。

【0101】

線形フィードバックシフトレジスタ44は、カウンタ43から信号“0”を受けると、この状態値 K_t を第2の鍵情報復号化部45に入力し、カウンタ43から信号“1”を受けると、この状態値 K_t から生成した次の状態値 K_{t+1} を第2の鍵情報復号化部45に入力する。

【0102】

第2の鍵情報復号化部45は、線形フィードバックシフトレジスタ44から受けた復号結果 K_t を鍵として、鍵情報制御部41から受けた暗号化データ $E_1(K_t)$ [KA] を復号し、得られた復号結果KA1を暗号アルゴリズム復号化部28bに入力する。

【0103】

暗号アルゴリズム復号化部28bは、この復号結果KA1を鍵として、暗号アルゴリズム格納部22から受けた暗号化データ $E_2(KA1)$ [A] を復号し、得られた復号結果A1を暗号化・復号化部24に入力する。

【0104】

以下、前述同様に、暗号化・復号化部24では、暗号アルゴリズム復号化部28bから受けた暗号アルゴリズムA1と、第1の鍵情報復号化部42から受けた鍵 K_{ij} とに基づいて、端末装置20本体から入力されるメッセージMを暗号化し、得られた暗号化データ $E(A1, K_{ij})$ [M] を他の端末装置jに送信する。

【0105】

また、暗号アルゴリズム復号化部28bは、線形フィードバックシフトレジスタ44から復号結果 K_{t+1} を受けた場合、この K_{t+1} を鍵として、鍵情報制御部41から受けた暗号化データ $E_2(K_t)$ [A] を復号し、復号結果としてランダムなデータ

(異なる鍵で復号されて得られた失敗データ)を暗号化・復号化部 2 4 に入力する。

【0 1 0 6】

この場合、暗号化・復号化部 2 4 では、メッセージ M を暗号化できず、エラーを出力する。

【0 1 0 7】

上述したように本実施形態によれば、鍵情報管理部 4 0 が、鍵情報格納部 2 1 b から暗号化データ E1(Kt) [KA1] が転送されたとき、この転送された回数をカウントしておき、転送回数が n 回以下のときには暗号化データ E1(Kt) [KA1] を復号して得られた復号鍵 KA1 を暗号化・復号化部 2 4 に入力するが、転送回数が n 回を越えたときには復号を失敗させて得たランダムなデータを暗号化・復号化部 2 4 に入力する。

【0 1 0 8】

このように、端末装置 2 0 i a が暗号アルゴリズムを使用する毎に、暗号アルゴリズムの復号鍵 KA1 の使用回数をカウントし、有効な使用回数を過ぎると、復号鍵 KA1 を更新して無効化させる構成としたので、暗号方式利用システムに用いられる暗号アルゴリズムを管理でき、暗号アルゴリズムの不正利用を阻止することができる。また、この手法は、端末装置 2 0 i b における記憶装置のバックアップによる暗号アルゴリズムの不正利用をも防ぐことができる。

【0 1 0 9】

なお、上記第 1 の実施形態では、毎回、復号鍵を要求する場合について説明したが、これに限らず、他の第 2 又は第 3 の実施形態と同様に制御部 2 5 と線形フィードバックシフトレジスタ 2 6 との間にカウンタを設け、1 回入手した復号鍵を使用する毎にカウンタで使用回数をカウントし、使用回数が n 回を越えたときに使用不可とし、再度、端末装置 2 0 i が要求を行う構成に変形しても、本発明を同様に実施して同様の効果を得ることができる。

【0 1 1 0】

同様に、上記第 2 又は第 3 の実施形態では、カウンタ 3 2, 4 3 を用いて使用回数をカウントし、使用回数が n 回を越えたときに使用不可とし、再度要求を行

う場合について説明したが、これに限らず、カウンタ 32, 43 を省略し、第 1 の実施形態と同様に、毎回、端末装置 20 i a, 20 i b が要求を行う構成に変形しても、本発明を同様に実施して同様の効果を得ることができる。

【0111】

また、上記各実施形態では、センタ装置 10, 10 a において、線形フィードバックシフトレジスタ 12 を用いて復号鍵 t を Kt に更新する場合について説明したが、これに限らず、線形フィードバックシフトレジスタ 12 に代えて、入力された値 t から所定の手順で Kt を生成可能な鍵生成装置（例、所定系列で乱数を生成可能な乱数生成器など）を用いた構成とし、且つ、端末装置 20 i, 20 i a ~ b において、線形フィードバックシフトレジスタ 26, 33, 44 に代えて、センタ装置 10, 10 a の鍵生成装置と同一内容の鍵生成装置を用いた構成としても、本発明を同様に実施して同様の効果を得ることができる。

【0112】

また、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、記憶媒体に格納して頒布することもできる。なお、この記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD 等）、光磁気ディスク（MO 等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0113】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働している OS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等の MW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【0114】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LAN やインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0115】

また、記憶媒体は 1 つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0 1 1 6】

また、ここで言うコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の 1 つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0 1 1 7】

また、係るコンピュータは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0 1 1 8】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0 1 1 9】

【発明の効果】

以上説明したように本発明によれば、暗号方式利用システムに用いられる暗号アルゴリズムを管理し、暗号アルゴリズムの不正利用を阻止し得る暗号方式管理システムを提供できる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態に係る暗号方式管理システムの構成を示すブロック図

【図 2】

同実施形態における暗号アルゴリズム管理部の構成を示すブロック図

【図 3】

本発明の第 2 の実施形態に係る暗号方式管理システムの構成を示すブロック図

【図 4】

同実施形態における暗号アルゴリズム管理部の構成を示すブロック図

【図 5】

本発明の第 3 の実施形態に係る暗号方式管理システムの構成を示すブロック図

【図 6】

同実施形態における暗号アルゴリズム管理部の構成を示すブロック図

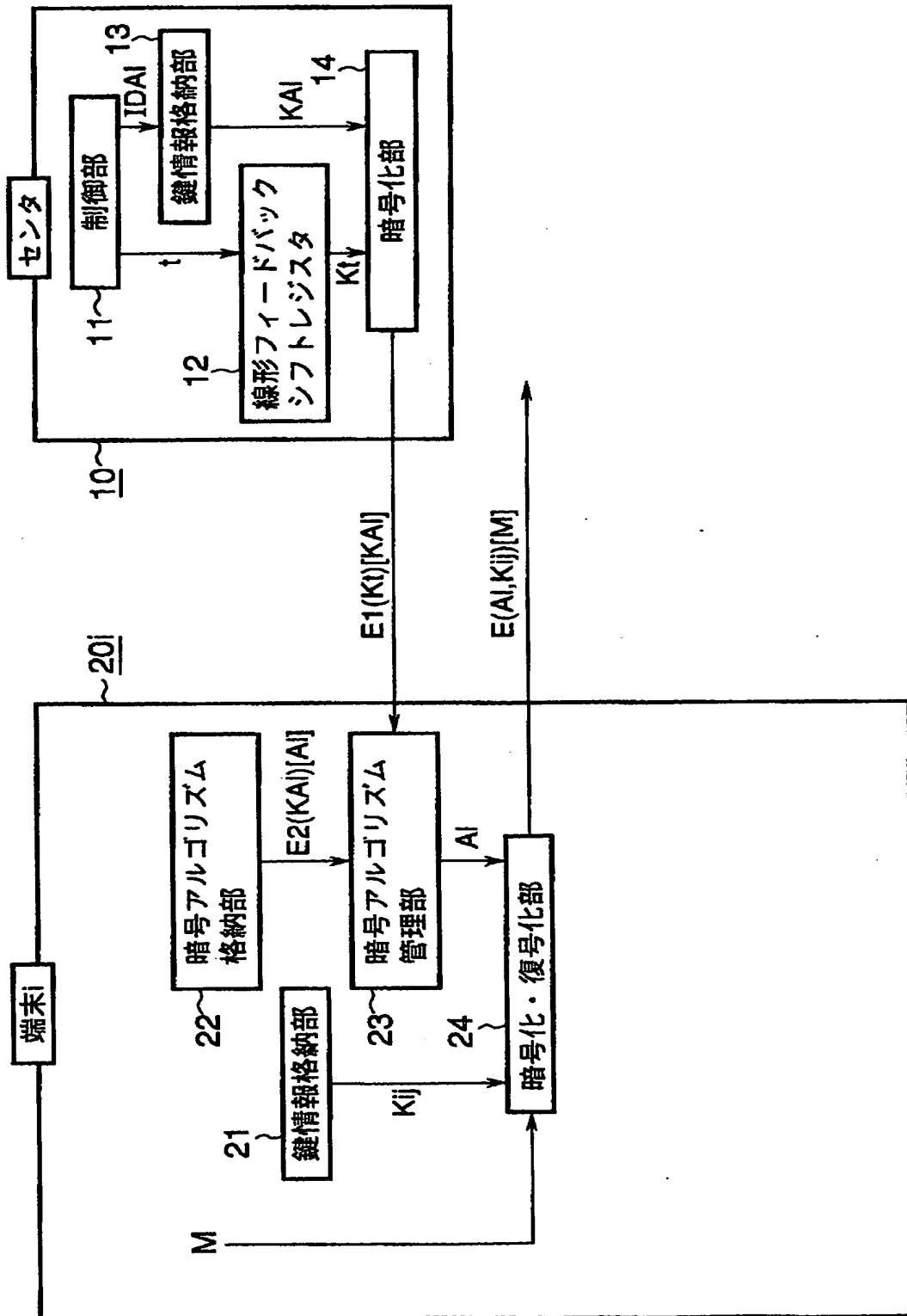
【符号の説明】

- 1 0, 1 0 a …センタ装置
- 1 1, 2 5, 3 1 …制御部
- 1 2, 2 6, 3 3, 4 4 …線形フィードバックシフトレジスタ
- 1 3, 2 1, 2 1 b …鍵情報格納部
- 1 4 …暗号化部
- 1 5 …暗号アルゴリズム格納部
- 2 0 i, 2 0 i a, 2 0 i b …端末装置
- 2 2 …暗号アルゴリズム格納部
- 2 3, 3 0 …暗号アルゴリズム管理部
- 2 4 …暗号化・復号化部
- 2 7, 4 2, 4 5 …鍵情報復号化部
- 2 8, 2 8 b, 3 4 …暗号アルゴリズム復号化部
- 3 2, 4 3 …カウンタ
- 4 0 …鍵情報管理部
- 4 1 …鍵情報制御部

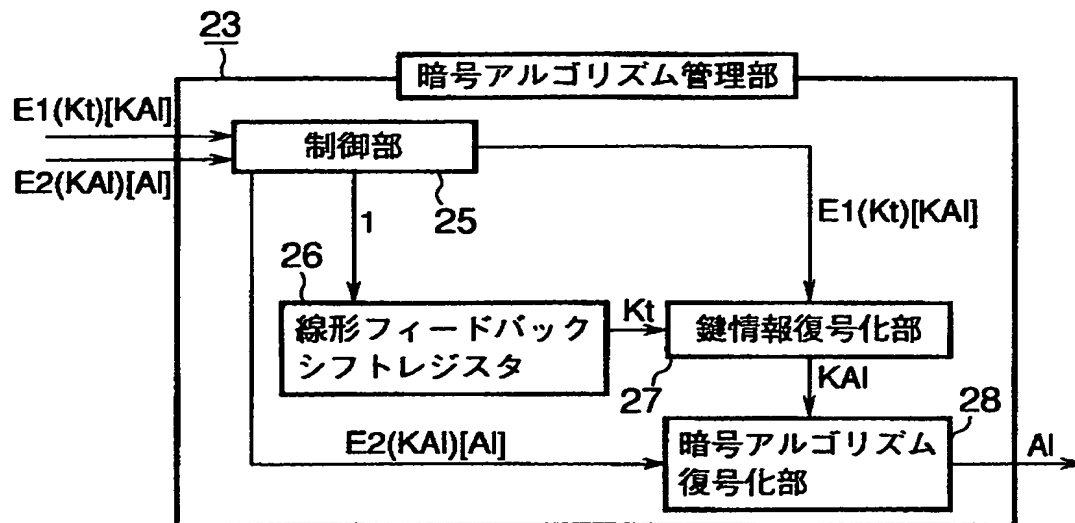
【書類名】

図面

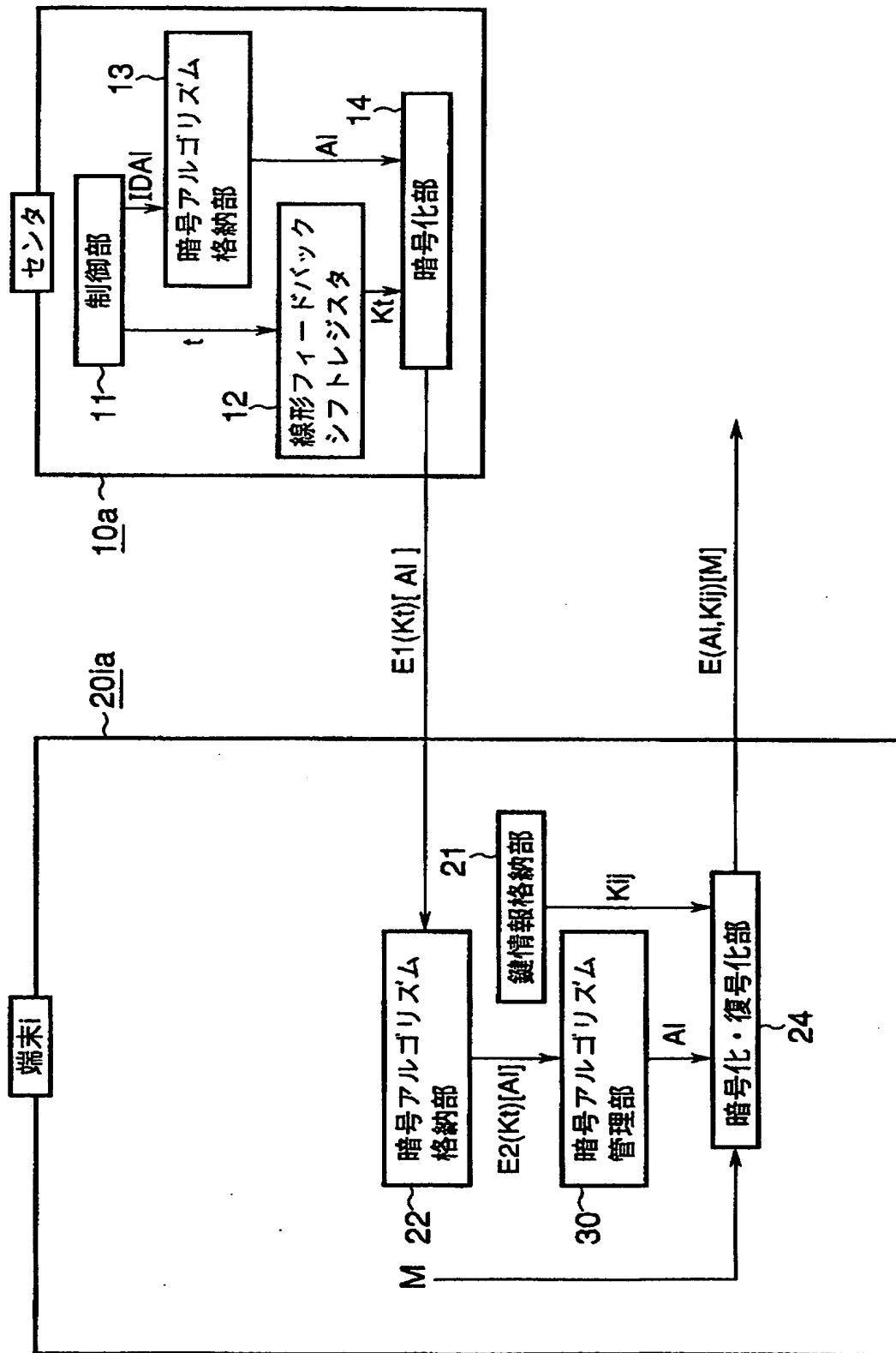
【図 1】



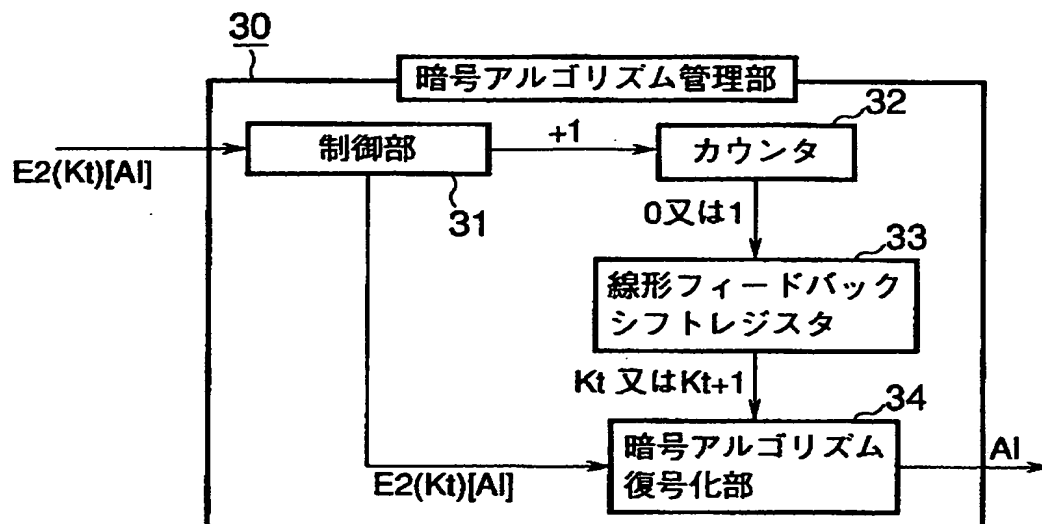
【図 2】



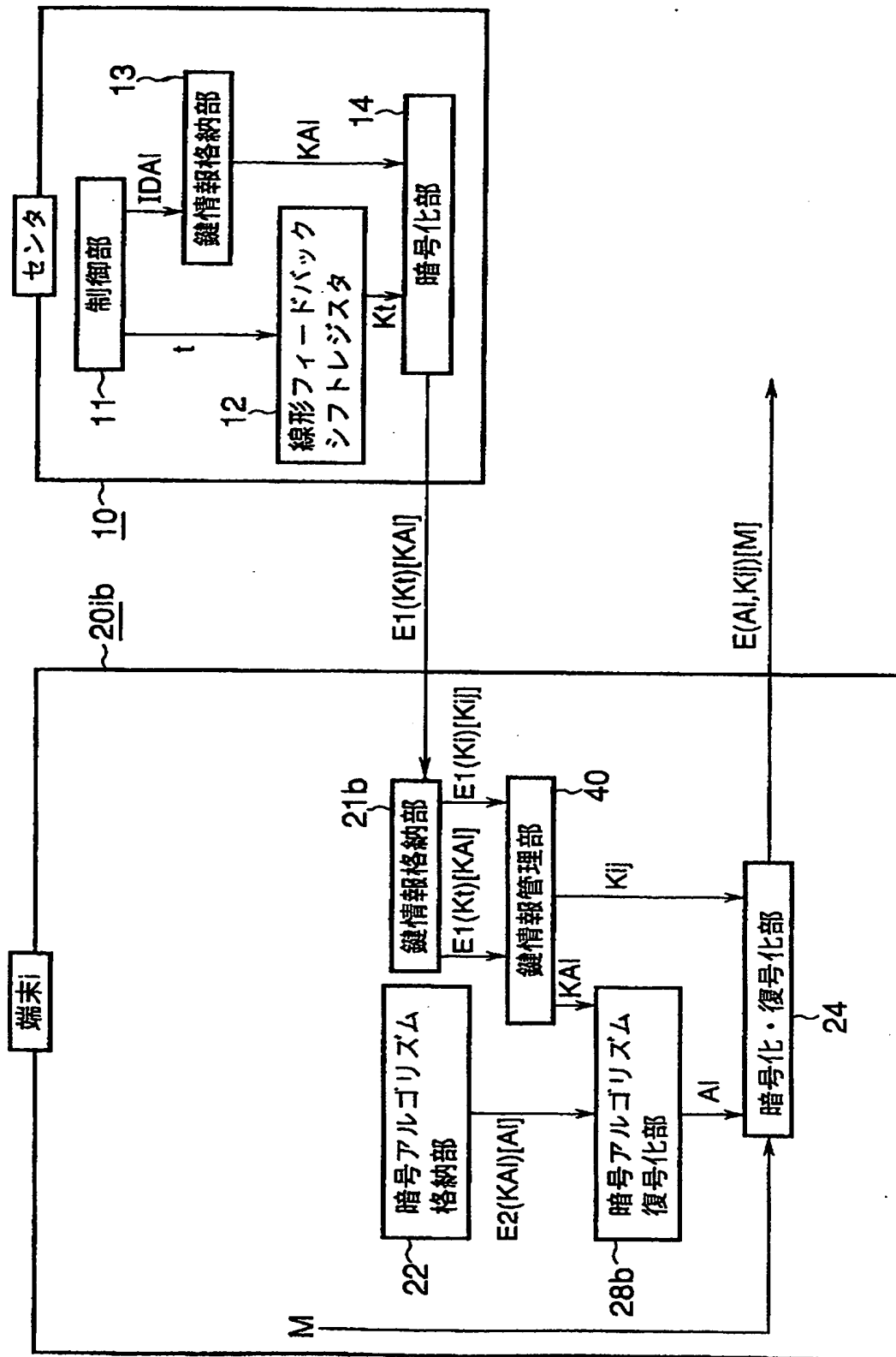
【図 3】



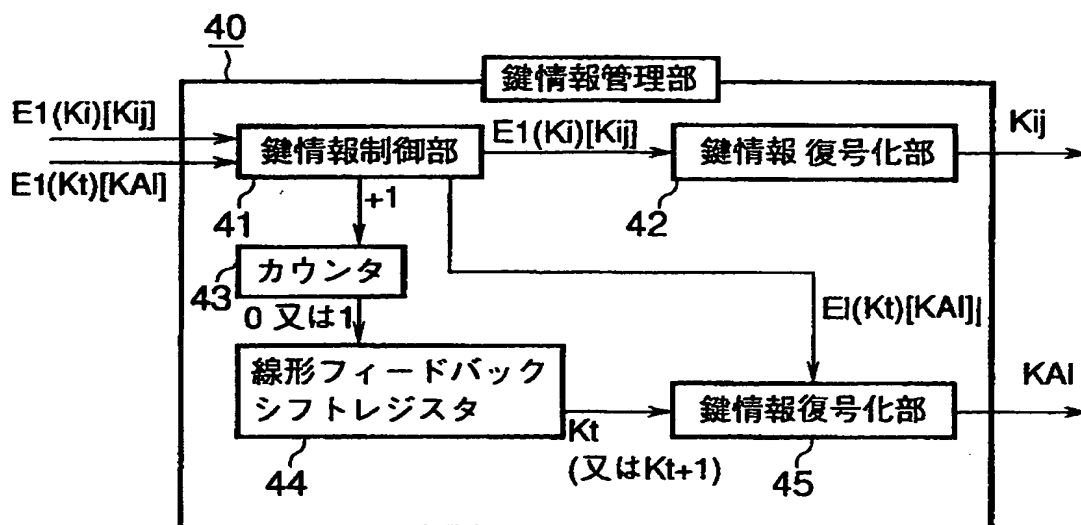
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 本発明は、暗号方式利用システムに用いられる暗号アルゴリズムを管理し、暗号アルゴリズムの不正利用の阻止を図る。

【解決手段】 端末装置 2 0 i では、暗号化された暗号アルゴリズムを復号する毎に、要求をセンタ装置に送信し、センタ装置では、要求を受けたとき、線形フィードバックシフトレジスタ 1 2 が、共有した状態値 t を更新し、暗号化部 1 4 が、更新された状態値 $K t$ に基づいて、暗号化された暗号アルゴリズムを復号可能な復号鍵を暗号化して得られた暗号化データを端末装置に返信し、端末装置では、暗号アルゴリズム管理部 2 3 が、センタ装置 1 0 から暗号化データを受けたとき、状態値 t を更新し、この更新された状態値 $K t$ に基づいて、暗号化データを復号し、得られた復号結果に基づいて、暗号アルゴリズムを出力する暗号方式管理システム。

【選択図】 図 1